http://infor.seaninstitute.org/index.php/infokum/index
JURNAL INFOKUM, Volume 9, No. 2, Juni 2021 ISSN : 2302-9706

Application of Integers in Vernam Cipher Cryptography (One Time Pad)

Parasian D.P Silitonga[1], Sorang Pakpahan[2]
[1]Informatics Engineering Study Program, Universitas Katolik Santo Thomas, [2]Information Systems Study Program, Universitas Katolik Santo Thomas.
parasianirene@gmail.com[1], sorangpakpahan@gmail.com[2]

Abstract

Article Info
Received 01 Juni 2021
Revised 10 Juni 2021
Accepted 30 Juni 2021

System security is currently an important concern. This is motivated by many business activities carried out through online transaction systems. A system with high security will certainly give high trust to users. By increasing the level of trust in the system, it directly adds to the value and usefulness of the system itself. There are several techniques that can be used to secure data on the system, one of which is cryptography. Data that is considered highly confidential will be disguised so that the data cannot be understood even though it can be read by unauthorized parties. Source data that has not been encrypted is known as plaintext, then after being disguised with plaintext it will turn into ciphertext.

Keywords: Cryptography, encryption, decryption, one time pad.

1. Introduction

Technological advances allow every human being and device to be connected in a virtual world or internet. Organizations and institutions, both state and private, such as educational, financial, health and other institutions. Advances in technology are realized to provide goodness, but on the other hand, technological advances have a negative effect. One of the negative effects of technological advances is the challenge to data security. The problem of data security is the background for the development of a data security system as well as an effort to protect data that is in the communication network. Today, the security of a system has become a risky matter for daily business activities. A system with a good level of security will be able to provide a level of trust to users so that it will directly add to the value and usability of the system.

Users will have a comfortable and safe feeling when dealing with the system. There are several techniques that can be done in an effort to produce a security process on a system. One technique that can be done is cryptography [1]. In cryptography, highly confidential data will be encoded so that although the data can be read and viewed, it will not be understood by unauthorized parties [2], [3]. The source of data that has not undergone the encryption process is known as plaintext, then after being subjected to this plaintext encoding process it will turn into ciphertext [4], [5]. The cryptographic method used in this study uses the Vernam Cipher Algorithm [6], [7].

Vernam Cipher Algorithm is one of the key algorithms[8]. Until now, the Vernam Cipher algorithm is still trusted as an encryption method, Vernam Cipher cryptography uses the same key for encryption and decryption[9]–[11].

2. Method

2.1. Data collection

The stages in this research method consist of several methods carried out as shown in the diagram below:

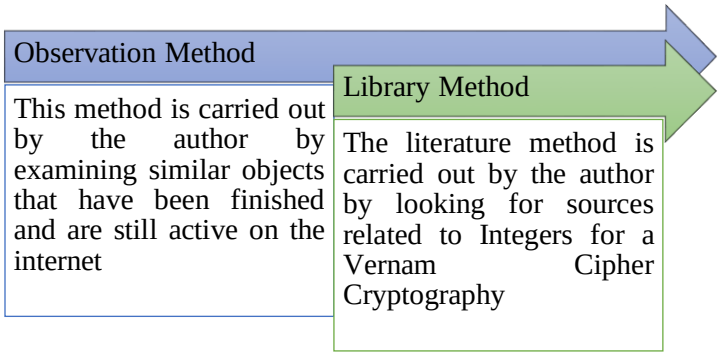

Figure 1. Stages of Data Collection

a. Observation Method
This method is carried out by the author by examining similar objects that have been finished and are still active on the internet.

b. Library Method
The literature method is carried out by the author by looking for sources related to Integers for a Vernam Cipher Cryptography, Studying books, literature, journals related to vernam cipher cryptography (One Time Pad).

2.2. Vernam Cipher Algorithm (One Time Pad)

The cipher method is implemented by using a key which is a series of characters that are generated randomly and do not repeat. Each key character is processed by adding modulo 26 with the characters in the data source. In the One Time Pad process, each key character is used once against one message and is not reused in another message. The length of the key character is the same as the length of the message to be encrypted. The only cryptographic algorithm that cannot be cracked is the one time pad. One-Time Pads (OTP). One time pads were invented in 1917 by Major Joseph Mauborgne. This cipher belongs to the group of symmetric cryptographic algorithms. One time pad (pad = notepad) contains a sequence of randomly generated key characters. Originally, a one time pad was a tape containing a sequence of key characters. One pad is only used once (one time) to encrypt a message, after that the pad that has been used is destroyed so that it is not used again to encrypt another message. The encryption rules used are exactly the same as in the Vigenere cipher. The sender of the message uses each character key to encrypt one plaintext character. Encryption can be described as a modulo 26 sum of one plaintext character with one key character one time pads: ci = (pi + ki) mod 26 which in this case, pi : plaintext character ki : key character ci : ciphertext character Note that the length of the key is equal to the length of the plaintext, so there is no need to reuse the key during the encryption process. After the sender has encrypted the message with one unit of time, it destroys the pad once (hence the name is used once). The recipient of the message uses one of the same timing pads to decrypt the ciphertext characters into plaintext characters with the equation : *pi = (ci – ki) mod 26*.

3. Results and Discussion

3.1 Key Formation in Round Month Cryptography

The following is the key formation process. This process is carried out by the recipient, in this case B.

1. Choose prime numbers p and q.
2. Calculate n = pq .
3. Calculate j (n) = (p -1)(q -1) .
4. Choose any number b, 1 < b <j (n) , with gcd(b,j (n)) = 1.
5. Calculate the inverse of b, i.e. a = b-1 modj(n) .
6. Public key: (n, b) and secret key: a.

In order to make it easier to understand the password with integers, specifically in this thesis, the plaintext used is only in the form of numbers 0 to 25 which correspond to the letters a to z. However, in actual use, correspondence tables such as ASCII codes are used, as well as very large numbers. In selecting p and q, n = pq must be greater than or equal to the possible plaintext values. In this case n = pq >= 25

Table 1. Frequency Patterns

A	B	C	D	E	F	D	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example:
B choose
p = 5
q = 11
n = p * q = 55
then n = 55
and R= (55) (5-1)(11-1) 4 x 10 40
choose any number (b) = 13
Then GCD =
gcd(13,40)
13 = 1.40 - 27
27 = 27.1
gcd = 1
so a = 13^1 mod 40
= 37
So the public key is (n,b) = (55,13) and the secret key is a = 37

3.2. One Time Pad

This research will discuss the analysis of the One Time Pad algorithm. For example, when sending a message to someone, the message must be confidential. In this discussion, One Time Pad will encrypt messages so that they are safe. Below will be explained an example of using the one time pad algorithm in a message.

For example: A message "UNIKA" will be encrypted with the key "XMCKL" with the following calculation, it will get the following results:

Table 2. Ascii Message

Plain Teks	Ascii
U	7
N	4
I	11
K	11
A	14

Table 3. Ascii Key

Teks Kunci	Ascii
X	23
M	12
C	2
K	10
L	11

From the table above it can be concluded as follows:
Message (plaintext) : 7(H) 4(E) 11(L) 11(L) 14(O)
Key : 23(X) 12(M) 2(C) 10(K) 11(L)

Key message	: 30	16	13	21	25

Messages are encrypted with mod 26
Message + mod key 26 : 4(E) 16(Q 13(N) 21(V) 25(Z)
Then it will produce encryption: **E Q N V Z**
To describe it, the reverse process is carried out, namely.

Ciphertext	: 4(E)	16(Q	13(N)	21(V)	25(Z
Key	: 23(X)	12(M)	2(C)	10(K)	11(L)
Ciphertext - key	:-19	4	11	11	14
Ciphertext - mod key 26:	7(U)	4(N)	11(I)	11(K)	14(A)

Then the encryption message will return to its original state: **UNIKA**

4. Conclusions

The application of integers in Vernam Cipher (One Time Pad) cryptography performs two processes, namely encryption and decryption. The process is very simple, but has weaknesses that might be developed and solved by other algorithms.

Reference

[1] H. Mukthar, *Kriptografi untuk Keamanan Data*. 2018.
[2] R. Watrianthos, "PERBANDINGAN TEKNIK KRIPTOGRAFI METODE SAPPHIRE II DAN RC4," *J. Inform.*, 2019, doi: 10.36987/informatika.v3i2.213.
[3] R. Munir, "Kriptografi," in *2*, 2019.
[4] W. Pramusinto, N. Wizaksono, A. Saputro, J. C. Raya, P. Utara, and K. Lama, "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman," *Vol .*, 2019.
[5] E. Rahmawan Pramudya, Abudussalam, and D. R. I. M. Setiadi, "Enkripsi Gambar Grayscale Menggunakan Kriptografi Rivest Cipher (RC) 4," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim 69*, 2018.
[6] A. A. Fikhri and H. Hendrawaty, "Implementasi Steganografi Text To Image Menggunakan Metode One Bit Least Significant Bit Berbasis Android," *J. Infomedia*, vol. 3, no. 1, pp. 10–17, 2018, doi: 10.30811/jim.v3i1.623.
[7] M. K. Harahap, "ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, 2016, doi: 10.30743/infotekjar.v1i1.43.
[8] D. Rizal, T. Sutojo, and Y. Rahayu, "Implementasi Kriptografi Gambar Menggunakan Kombinasi Algoritma Elgamal Dan Mode Operasi Ecb (Electronic Code Book)," *Techno.COM*, 2016.
[9] N. M. D. Oktafiansyah, F. Agus, and S. Maharani, "Penerapan Kriptografi Dengan Algoritma Data Encryption Standart Pada Text Hasil Konversi Dari Citra," *Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 1, no. 1, pp. 85–89, 2016.
[10] D. Adhar, "Implementasi Algoritma Des (Data Encryption Standard) Pada Enkripsi Dan Deskripsi Sms Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 53–60, 2019, [Online]. Available: https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/185.
[11] S. Wardoyo and R. Fahrizal, "Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android," *Setrum Sist. Kendali-Tenaga-elektronika-telekomunikasi-komputer*, vol. 3, no. 1, p. 43, 2016, doi: 10.36055/setrum.v3i1.497.